PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-006710
(43)Date of publication of application : 10.01.1997

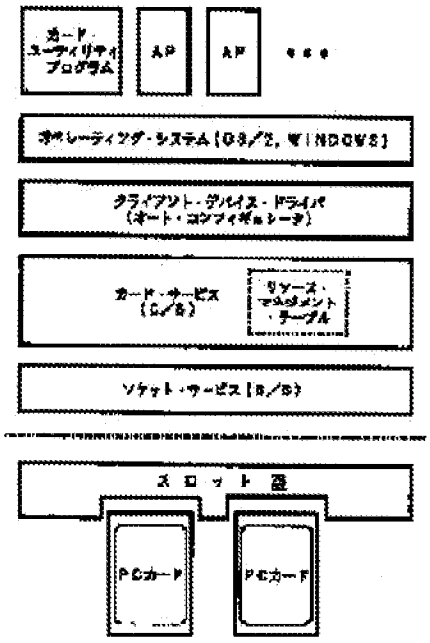
(51)Int.Cl. G06F 13/14
G06F 1/26
G06F 1/00
G06F 13/00
G06K 17/00

(21)Application number : 07-155681
(22)Date of filing : 22.06.1995

(71)Applicant : INTERNATL BUSINESS MACH CORP <IBM>
(72)Inventor : OSHIYAMA TAKASHI
SHINOMURA MASAHIKO

(54) INFORMATION PROCESSOR AND ITS CONTROL METHOD

(57)Abstract:
PURPOSE: To prevent the generation of illicit intrusion from a loaded device into an information processor by stopping power supply to the loaded device when a security mode is selected.
CONSTITUTION: When the setting of the security mode is instructed, a card utility program requests the issuance of a false card removal event to card service. At the time of receiving the request, a client device driver has an illusion that a PC card has been ejected and opens the resource of a card slot 26. Then the card utility program informs the card service of the setting of the security mode together with a pass word. Therefor even when the PC card is reinserted into the slot 26 in the security mode, the card service neglects the insertion of the card and does not transmit an event indicating the insertion of the PC card to the client device driver.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平9－6710

(43)公開日　平成９年(1997)１月10日

(51)Int.Cl.°		識別記号	庁内整理番号	Ｆ Ｉ			技術表示箇所
Ｇ０６Ｆ	13/14	３３０	7368－5E	Ｇ０６Ｆ	13/14	３３０Ｄ	
	1/26				1/00	３７０Ｅ	C7
	1/00	３７０			13/00	３０１Ｒ	
	13/00	３０１		Ｇ０６Ｋ	17/00	Ｂ	
Ｇ０６Ｋ	17/00					Ｅ	

審査請求　未請求　請求項の数17　ＯＬ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平7－155681

(22)出願日　平成７年(1995)６月22日

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504，ニューヨーク州　アーモンク　（番地なし）

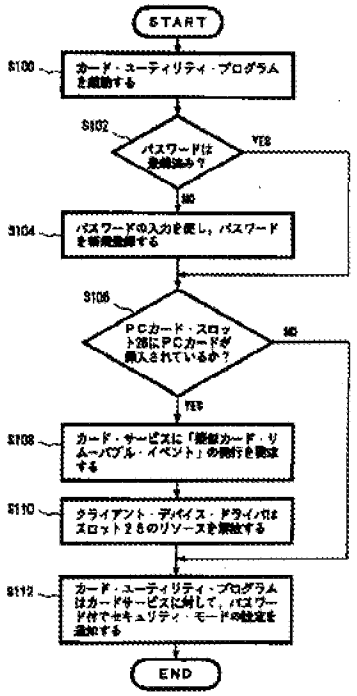
(72)発明者　押　山　隆
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内

(74)代理人　弁理士　合田　潔　（外２名）

最終頁に続く

(54)【発明の名称】　情報処理装置及びその制御方法

(57)【要約】
【目的】　装着されたＰＣカードからパーソナル・コンピュータ内部への不正な侵入（すなわち機密データへのアクセス）を好適に防止する。
【構成】　パーソナル・コンピュータは、セキュリティ・モードに遷移すると、現実のデバイスの装着の有無に拘らず、あたかもデバイスが装着されていないかのように擬似的に振る舞うようになっている。したがって、所定の動作モード下では、装着されたデバイスには電力を供給せず、該デバイスは活動化しないことになる。この間は、当然、装着されたデバイスと情報処理装置は互いに交信することはできない。



1

【特許請求の範囲】

【請求項１】デバイスを装着するための接続部を持ち、且つ装着されたデバイスに対して電力を供給するタイプの情報処理装置において、所定の動作モード下では、装着されたデバイスに対する電力供給を停止可能なことを特徴とする情報処理装置

【請求項２】デバイスを装着するための接続部を持ち、且つ該接続部へのデバイスの装着を検出すると該デバイスに電力供給を行うタイプの情報処理装置において、所定の動作モード下では、デバイスの装着の有無に拘らず該接続部からの電力供給を停止することを特徴とする情報処理装置

【請求項３】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持ち、該検出部の検出結果に応じて装着されたデバイスに電力供給を行うタイプの情報処理装置において、所定の動作モード下では、前記検出部の検出結果に拘らず擬似的にデバイスが装着されていないと判断してデバイスへの電力供給を停止することを特徴とする情報処理装置

【請求項４】デバイスを装着するための接続部を持ち、且つ装着されたデバイスとの間で交信可能なタイプの情報処理装置において、所定の動作モード下では、装着されたデバイスとの交信を禁止することを特徴とする情報処理装置

【請求項５】デバイスを装着するための接続部を持ち、且つ該接続部へのデバイスの装着を検出すると該デバイスとの交信が可能になるタイプの情報処理装置において、所定の動作モード下では、デバイスの装着の有無に拘らずデバイスとの交信を禁止することを特徴とする情報処理装置

【請求項６】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持ち、該検出部の検出結果に応じて装着されたデバイスとの交信が可能になるタイプの情報処理装置において、所定の動作モード下では、前記検出部の検出結果に拘らず擬似的にデバイスが装着されていないと判断して交信を禁止することを特徴とする情報処理装置

【請求項７】入力されたパスワードの照合結果に応じて前記所定の動作モードに遷移することができることを特徴とする請求項１乃至請求項６のいずれかに記載の情報処理装置

【請求項８】入力されたパスワードの照合結果に応じて前記所定の動作モードから抜け出すことができることを特徴とする請求項１乃至請求項６のいずれかに記載の情報処理装置

【請求項９】前記所定の動作モードとは機密保護性の高いセキュリティ・モードであることを特徴とする請求項１乃至請求項６のいずれかに記載の情報処理装置

【請求項１０】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部

2

を持つタイプの情報処理装置の制御方法において、所定の動作モード下では、前記検出部の検出結果に拘らず前記接続部にはデバイスが装着されていないものと判断することを特徴とする情報処理装置の制御方法

【請求項１１】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持つタイプの情報処理装置の制御方法において、所定の動作モード下では、前記検出部の検出結果に拘らず前記接続部にはデバイスが装着されていないものと判断して、装着されたデバイスへの電力供給を停止することを特徴とする情報処理装置の制御方法

【請求項１２】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持つタイプの情報処理装置の制御方法において、所定の動作モード下では、前記検出部の検出結果に拘らず前記接続部にはデバイスが装着されていないものと判断して、装着されたデバイスとの交信を禁止することを特徴とする情報処理装置の制御方法

【請求項１３】入力されたパスワードの照合結果に応じて前記所定の動作モードに遷移することができることを特徴とする請求項１０乃至請求項１２のいずれかに記載の情報処理装置の制御方法

【請求項１４】入力されたパスワードの照合結果に応じて前記所定の動作モードから抜け出すことができることを特徴とする請求項１０乃至請求項１２のいずれかに記載の情報処理装置の制御方法

【請求項１５】前記所定の動作モードとは機密保護性の高いセキュリティ・モードであることを特徴とする請求項１０乃至請求項１２のいずれかに記載の情報処理装置の制御方法

【請求項１６】パスワードの入力に所定回数以上失敗すると前記所定の動作モードの解除を禁止してしまうことを特徴とする請求項７に記載の情報処理装置

【請求項１７】パスワードの入力に所定回数以上失敗すると前記所定の動作モードの解除を禁止してしまうことを特徴とする請求項１４に記載の情報処理装置の制御方法

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、パーソナル・コンピュータなどのようにデバイス（例えばＰＣカード）を拡張することができる情報処理装置及びその制御方法に係り、特に、デバイスを拡張したときの機密保護を実現できる情報処理装置及びその制御方法に関する。更に詳しくは、本発明は、デバイスを拡張したときのソフトウェア・レベルでの機密保護を実現できる情報処理装置及びその制御方法に関する。

【０００２】

【従来の技術】昨今の技術革新に伴い、デスクトップ型、ノートブック型など各種パーソナル・コンピュータ

が開発され市販されている。

【0003】このようなパーソナル・コンピュータ（以下、「PC」ともいう）は、小型に設計されており、出荷時に標準装備することが可能な周辺機器類（システム・メモリや入出力装置、補助記憶装置など）の個数には限界がある。したがって、ユーザの多くは、PCを購入後、自らの手で必要とするデバイスを拡張して、コンピュータの機能強化を図っている。

【0004】デスク・トップ型やタワー型コンピュータのようにPC本体内の収容スペースに余裕がある機種の場合、デバイスの拡張は、所望のアダプタ・カード（「オプション・カード」又は「拡張ボード」ともいう）をシステム・ボート上の拡張スロットに挿し込む、という形態で行われていた（図7(a)参照）。ビデオ・アダプタ，通信用アダプタ，フロッピー・ディスク・インターフェース，ハード・ディスク・インターフェース，シリアル・インターフェース，パラレル・インターフェース，増設メモリ，SCSI（Small Computer System Interface）インターフェースなどが、アダプタ・カードの最たる例である。

【0005】一方、ノートブック・コンピュータの場合、筐体内の実装密度が極度に高く、スペースにゆとりがないので、アダプタ・カードの装着は実用的ではない。（デスクトップ／タワー型のPCでは10個以上の拡張スロットをもつ製品もあるのに対して、ラップトップ型やノートブック型のPCは、拡張スロットが全く用意されていないかあっても小型のものが1、2個程度に過ぎない。）

【0006】いわゆるPCカードは、収容スペースに制限のあるノートブック・コンピュータの拡張性を補うために開発された、クレジット・カード・サイズの拡張デバイスである（図7(b)参照）。PCカードのハードウェア的（すなわち機械的及び電気的）なガイドラインは、米PCMCIA（Personal Computer Memory Card International Association）やJEIDA（日本電子工業振興協会）が中心となって、国際標準として策定されている。現在、3．3㎜厚のType1，5．5㎜厚のType2，10．5㎜厚のType3、という3種類のPCカードが用意されている。Type1は主にメモリ・カードとして利用されている。Type2はファクシミリ・モデムやEthernetアダプタ、SCSIアダプタなどの用途に使われている。また、Type3は主にハード・ディスク内蔵カードとして利用されている。このようなPCカードは、電子部品の小型化技術などによってもたらされたものであり、ノートブック・コンピュータの小型化、軽量化、省電力化、可搬性の要求に適ったものでもある。1993年にPCMCIA Re2．1／JEIDA4．2が世界標準として採択されてからPCカードの普及は急速に加速された。現在、殆どのノートブック・コンピュータがPCカード用スロットを標準的に備えている。また、有益なPCカードの用途をノートブック・コンピュータに限定する理由はなく、最近では、PCカード用スロットを持つデスクトップ型PCも増えてきた（例えば、IBM PC（パーソナル・コンピュータ）720やIBM PC750は、デスクトップ型ではあるが、PCカード用スロットを備えている）。1994年夏に米国政府が「全てのデスクトップPCにPCカード用スロットを装備すること」を調達基準として打ち出したことから、ノートブックPCのみならずデスクトップPCもPCカードの大きな市場となりつつある。価格面では、今のところアダプタ・カードよりもPCカードの方が割高であるが、PCカードの市場が広がれば、量産効果でアダプタ・カード以下の価格になる可能性も大きい。

【0007】最近では、このようなPCカードの市場拡大の波により、従来軽視されがちであったPCカードの機密保護（セキュリティ）の問題がクローズ・アップされるようになってきた。

【0008】本出願人に譲渡されている特願平05－182972号明細書（特開平07－44269号公報：当社整理番号JA9－93－030）には、ノートブックPCに装着されたPCカードの無断取り出しをロックするための機構について開示されている。同明細書に係るPCカード・ロック機構は、より詳細には、PC本体の側面にPCカード用スロットを備え且つキーボードをPC本体に対して開閉自在なノートブックPCにおいて、キーボードを開放した際にPCカードの取り出しを規制するための係止片を挿入し、その後キーボードを閉じてロックすることによって、イジェクト・ボタンの操作に拘らずPCカードの抜き取りを物理的に禁止できる、というものである（図8参照）。このようなキーボード・ロックと連動するPCカード・ロック機構は、例えば、日本アイ・ビー・エム（株）が市販するThinkPad750及び755にも既に用いられている（"ThinkPad"は米IBM社の商標）。

【0009】ところが、最近では、PCカード自体の盗難など物理的な（若しくはハードウェア・レベルでの）セキュリティだけではなく、データの不正コピー、誤った使用方法に因るデータの破損など、ソフトウェア・レベルでのセキュリティも考慮しなければならなくなってきた。

【0010】PCMCIA／JEIDAが新しく規定した1995年版の規格"PC Card Standard"によれば、PCカードの内部バスを、従来のISA（Industry Standard Architecture）バス・ベースの16ビット幅から、"CardBus"と呼ばれる32ビット幅のものに拡張して、さらにバスの動作クロック速度を33MHzに高速化することになっている。その瞬間的な最大転送速度は132Mbpsに到達し、PCI（Peripheral Component Interconnect）バスの性能に

5

相当する。これに伴って、ＣＰＵ内蔵型カード，高速な記憶カード，グラフィックスや動画を扱えるマルチメディア・カードなど、より高機能なＰＣカードが急速に普及することが見込まれる。特にＣＰＵ内蔵型カードは、ＰＣ本体内のシステム・バスの占有権を握ることができる「バス・マスタ」にもなり得る。ハッカーらにとっては、このようなＰＣカードを使ってコンピュータ・システム内部に侵入し、ひいてはデータを盗み出すためのツールを作成することは、以前に比べて極めて容易になってくる。したがって、ソフトウェア・レベルでのＰＣカード・スロットのセキュリティ維持は、システムの資産保護の観点から、益々重要性を増してきているのである。

【００１１】

【発明が解決しようとする課題】本発明の目的は、パーソナル・コンピュータなどのようにデバイス（例えばＰＣカード）を拡張することができる、優れた情報処理装置及びその制御方法を提供することにある。

【００１２】本発明の更なる目的は、デバイスを拡張したときの機密保護を実現できる情報処理装置及びその制御方法を提供することにある。

【００１３】本発明の更なる目的は、デバイスを拡張したときのソフトウェア・レベルでの機密保護を実現できる情報処理装置及びその制御方法を提供することにある。

【００１４】本発明の更なる目的は、装着されたＰＣカードから情報処理装置内部への不正な侵入（すなわち機密データへのアクセス）を好適に防止することができる情報処理装置及びその制御方法を提供することにある。

【００１５】本発明の更なる目的は、装着されたＰＣカードから情報処理装置内部へのアクセスに対して、ソフトウェア・レベルで機密保護を実現できる情報処理装置及びその制御方法を提供することにある。

【００１６】

【課題を解決するための手段及び作用】本発明は、上記課題を参酌してなされたものであり、その第１の側面は、デバイスを装着するための接続部を持ち、且つ装着されたデバイスに対して電力を供給するタイプの情報処理装置において、所定の動作モード下では、装着されたデバイスに対する電力供給を停止可能なことを特徴とする情報処理装置である。

【００１７】また、本発明の第２の側面は、デバイスを装着するための接続部を持ち、且つ該接続部へのデバイスの装着を検出すると該デバイスに電力供給を行うタイプの情報処理装置において、所定の動作モード下では、デバイスの装着の有無に拘らず該接続部からの電力供給を停止することを特徴とする情報処理装置である。

【００１８】また、本発明の第３の側面は、デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持ち、該検出部の検出結果に応じて装着されたデバイスに電力供給を行うタイプの情報処理装置において、所定の動作モード下では、前記検出部の検出結果に拘らず擬似的にデバイスが装着されていないと判断してデバイスへの電力供給を停止することを特徴とする情報処理装置である。

6

【００１９】また、本発明の第４の側面は、デバイスを装着するための接続部を持ち、且つ装着されたデバイスとの間で交信可能なタイプの情報処理装置において、所定の動作モード下では、装着されたデバイスとの交信を禁止することを特徴とする情報処理装置である。

【００２０】また、本発明の第５の側面は、デバイスを装着するための接続部を持ち、且つ該接続部へのデバイスの装着を検出すると該デバイスとの交信が可能になるタイプの情報処理装置において、所定の動作モード下では、デバイスの装着の有無に拘らずデバイスとの交信を禁止することを特徴とする情報処理装置である。

【００２１】また、本発明の第６の側面は、デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持ち、該検出部の検出結果に応じて装着されたデバイスとの交信が可能になるタイプの情報処理装置において、所定の動作モード下では、前記検出部の検出結果に拘らず擬似的にデバイスが装着されていないと判断して交信を禁止することを特徴とする情報処理装置である。

【００２２】また、本発明の第７の側面は、デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持つタイプの情報処理装置の制御方法において、所定の動作モード下では、前記検出部の検出結果に拘らず前記接続部にはデバイスが装着されていないものと判断することを特徴とする情報処理装置の制御方法である。

【００２３】また、本発明の第８の側面は、デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持つタイプの情報処理装置の制御方法において、所定の動作モード下では、前記検出部の検出結果に拘らず前記接続部にはデバイスが装着されていないものと判断して、装着されたデバイスへの電力供給を停止することを特徴とする情報処理装置の制御方法である。

【００２４】また、本発明の第９の側面は、デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持つタイプの情報処理装置の制御方法において、所定の動作モード下では、前記検出部の検出結果に拘らず前記接続部にはデバイスが装着されていないものと判断して、装着されたデバイスとの交信を禁止することを特徴とする情報処理装置の制御方法である。

【００２５】しかして、本発明に係る情報処理装置及びその制御方法によれば、「所定の動作モード」に遷移すると、情報処理装置は、現実のデバイスの装着の有無に

拘らず、あたかもデバイスが装着されていないかのように擬似的に振る舞うようになっている。したがって、所定の動作モード下では、装着されたデバイスには電力を供給せず、該デバイスは活動化しないことになる。この間は、当然、装着されたデバイスと情報処理装置は互いに交信することはできない。要するに、装着されたＰＣカードから情報処理装置内部への不正な侵入（すなわち機密データへのアクセス）を好適に防止することができる訳である。また、装着されたＰＣカードから情報処理装置内部へのアクセスに対するこのような機密保護オペレーションは、ソフトウェア・プログラムによっても実現されるのである。

【００２６】なお、ここでいう「所定の動作モード」とは、機密保持性の高い「セキュリティ・モード」のことである。

【００２７】情報処理装置がセキュリティ・モードに遷移する際には、ユーザ（若しくはオペレータ）に対してパスワードの入力を求めるようにしてもよい。また、情報処理装置がセキュリティ・モードから抜け出す際にも、ユーザ（若しくはオペレータ）に対してパスワードの入力を求めるようにしてもよい。セキュリティ・モードを解除する際、ユーザが所定回数（例えば３回）以上パスワードの入力に失敗すると、パスワードの再入力だけでなく、セキュリティ・モードの解除自体を不能にしてしまうようにしてもよい。このようにすれば、オーソライズされていないユーザが許可なくセキュリティ・モードを解除して、デバイス側から情報処理装置内の機密データに不正にアクセスすることを厳しく禁止することができる訳である。

【００２８】本発明に係るセキュリティ・モードは、情報処理装置本体が、現実のデバイスの装着の有無に拘らず、デバイスを装着していないと擬似的に認識することによって実現される。当然、装着されたデバイス（例えばＰＣカード）側ではなく、情報処理装置本体側が該モードの設定・解除を管理するものであり、デバイス側からは勝手に解除することはできない。したがって、不正なユーザが勝手にデバイスを差し替えても情報処理装置内部に侵入することはできない。

【００２９】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３０】

【実施例】以下、図面を参照しながら本発明の実施例を詳解する。

【００３１】A．パーソナル・コンピュータ（ＰＣ）のハードウェア構成

図１には、本発明の実施に供されるパーソナル・コンピュータ（ＰＣ）１０のハードウェア構成を示している。

【００３２】ＰＣ１０内では、メイン・コントローラであるＭＰＵ（Micro Processing Unit）１１が、オペレーティング・システム（ＯＳ）の制御下で、各種アプリケーション・プログラムを実行するようになっている。ＭＰＵ１１は、データ信号線、アドレス信号線、コントロール信号線などからなる共通信号伝送路（「バス」ともいう）１２を介して各部と連絡している。

【００３３】メイン・メモリ１３は、ＯＳやアプリケーション・プログラムなど各ソフトウェアをロードしたり、ＭＰＵ１１が作業領域として用いたりするための書き込み可能な揮発性メモリ（ＲＡＭ）である。メイン・メモリ１３には、大容量を比較的安価で入手可能なダイナミックＲＡＭ（ＤＲＡＭ）が用いられる。メモリ・コントローラ１４は、メイン・メモリ１３へのアクセス動作を制御するためのものである。ＲＯＭ１５は、製造時に書き込みデータを決めてしまう不揮発性メモリであり、システムの始動時に行うテスト・プログラム（ＰＯＳＴ）や、システム内の各ハードウェアを制御するためのプログラム（ＢＩＯＳ）などをコード化して半永久的に格納するために用いられる。

【００３４】ビデオ・コントローラ１６は、ＭＰＵ１１からの描画命令を実際に処理するための周辺コントローラであり、処理した描画情報を画面バッファ（ＶＲＡＭ）１７に一旦書き込むとともに、ＶＲＡＭ１７から描画情報を読みだして表示装置（例えば液晶表示装置（ＬＣＤ））１８に出力するようになっている。

【００３５】ハード・ディスク・ドライブ（ＨＤＤ）１９やフロッピー・ディスク・ドライブ（ＦＤＤ）２０は、いわゆる補助記憶装置であり、ソフトウェアや作成データなどの保管に用いられる。フロッピー・ディスク・コントローラ（ＦＤＣ）２１は、ＦＤＤ２０駆動用の専用コントローラである。ＨＤＤ１９、ＦＤＤ２０へのアクセスは、一般には、オペレーティングシステム内のファイル管理サブシステムによって管理されている。

【００３６】キーボード／マウス・コントローラ（ＫＭＣ）２２は、キーボード２３からの入力マトリックスや、マウス２４からの座標指示入力を処理するための周辺コントローラである。

【００３７】ＰＣＭＣＩＡコントローラ（"ＰＣＩＣ"ともいう）２５は、ＰＣ１０本体側（以下、「ホスト」ともいう）とＰＣカード間でのシグナルの授受を可能にするためのコントローラ・チップであり、ＰＣカードのレジスタやＩ／Ｏ空間を低レベルで（すなわち電気的に）制御するようになっている。ＰＣＭＣＩＡコントローラ２５のローカル側には、ＰＣカードを収容するためのＰＣカード用スロット２６が配設されている。ＰＣカード用スロット２６は、例えばＴｙｐｅ１／２を２枚、又はＴｙｐｅ３を１枚だけ装着できるタイプでもよい。

【００３８】なお、ＰＣ１０は、図１に示した以外にも、当業者には周知の多くの電気回路や周辺機器等を含んでいるが、本発明の要旨を説明する上では不要ゆえ、本明細書では省略してある。

【0039】B．パーソナル・コンピュータ（PC）とPCカードとの連絡

図2には、PC10本体とPCカードとを連絡するためのハードウェア構成を、より詳細に描いている。PCカードは、機械的にはPCカード用スロット26に装着され、電気的には、PCMCIAコントローラ25を介してホスト側のバス12と連絡している。なお、バス12は、例えばISA（industry StandardArchitecture）バスでもよい。

【0040】PCMCIAコントローラ25は、ホストとPCカード間でのシグナルの授受を可能にするためのコントローラ・チップであり、ホスト側のバス12とはインターフェース部31を介して連絡しており、また、PCカード側とはドライバ部34及びレシーバ部35を介して連絡している。

【0041】インターフェース部31は、バス12のアドレス・バス，データ・バス，コントロール・バスと結ばれており（アドレス・バスはホストからの一方向のみ、データ・バス及びコントロール・バスは双方向）、ホスト側とPCカードとの間での動作タイミングの調整やデータの表現形式の変換などを行うようになっている。

【0042】ドライバ部34は、コントロール・バスが示す制御内容に従ってPCカードを駆動するための回路である。レシーバ部35は、逆にPCカード側からの帰路データを受け取ってインターフェース回路31に渡すための回路である。

【0043】レジスタ部32は、特定のデータを一時的に格納するための回路であり、インターフェース部31からアドレス・バス及びデータ・バスの一部を入力している。レジスタ部32は、ホスト側から受け取ったシステム・コンフィギュレーションに関する指定値（例えばI／Oアドレス，IRQレベル，DMAレベルなど）を書き込むためのアドレス、PCカード用スロット26へのカードの装着状況を書き込むためのアドレス、PCカード用スロット26への電力供給の有無に関する指示（V_{cc} ビット及びV_{pp} ビット）を書き込むためのアドレスなどを含んでいる。図3には、レジスタ部32の内部構成を模式的に示している。同図では、m番地は電力供給を制御するためのV_{cc} ビット及びV_{pp} ビットのために割り当てられ、また、n番地はカード装着の有無を書き込むために割り当てられている。PCカードのカード・スロット26への着脱は、PCカードの特定のコネクタ・ピン（仮に"Card Detect"ピンと呼ぶ）の電圧レベルを読み取ることによって検出され（周知）、その結果がレジスタ部32のn番地に書き込まれる。ホスト側は、I／Oリード・サイクルにより又はポーリングによって、レジスタ部23の各アドレスにアクセスして、PCカードの装着を検知したりカード・スロット26への電力供給を指示したりすることができる。

【0044】PCMCIA／JEIDAの策定した標準仕様によれば、PC本体側はPCカードに対してV_{cc} とV_{pp} という2系統の電源電圧を供給することになっている。V_{cc} はPCカードが通常のオペレーションを行うための基準電圧（3．3V又は5V）を与えるものであり、V_{pp} は比較的高い電圧（12V）を要するアップグレード・オペレーション（例えばフラッシュ・メモリの消去／書き込み動作）をサポートするためのものである。本実施例では、PCMCIAコントローラ25内の電源管理部33が電源電圧V_{cc} 及びV_{pp} の供給／停止を制御するようになっている。すなわち、電源管理部33は、各電源V_{cc} 及びV_{pp} をカード・スロット26に接続／遮断するためのFETスイッチ36，37の各ゲートに制御信号を出力しており、レジスタ部32のV_{cc} ビット及びV_{pp} ビットを参照して、各ビットの内容に応じてFETスイッチ36，37を付勢し又は滅勢するようになっている。なお、FETスイッチ36，37はPチャネル型でもNチャネル型MOSFETでもよく、また、MOS　FETではなくバイポーラ型トランジスタでもよい。

【0045】C．パーソナル・コンピュータ（PC）のソフトウェア構成

図4には、本発明をインプリメントしたPC10のソフトウェア構成を示している。HDD19やFDD20などからメイン・メモリ13にロードされた各プログラムは、同図に示すような階層構造に模式化して把握することができよう。

【0046】ソフトウェア層の最下層はソケット・サービス（S／S）である。ソケット・サービスは、PCMCIAコントローラ25に直接アクセスして制御するためのファンクション・コールを備えた統一的なインターフェースである。各メーカが提供するPCMCIAコントローラは、アクセス方式や活線挿抜に対する電源立上げサポートなどの点で仕様が異なるが、ソケット・サービスはこれらの相違を吸収する役目も果たす。ソケット・サービスは、例えばI／O・サイクルを利用することによってPCMCIAコントローラ25内のレジスタ部32の所定番地にアクセスして、その内容を読みだしたり書き込んだりすることができる。カード・サービス（後述）等の上位のソフトウェアは、このソケット・サービスを通じて、スロット26の状態などを取得することができる。

【0047】カード・サービス（C／S）は、PCカードの入出力のためにそのリソースを管理するデバイス・ドライバであり、ソケット・サービスの直近上位に位置し、ソケット・サービスに対してファンクション・コールを発行するとともに、より上位のソフトウェア（例えば後述の「クライアント・デバイス・ドライバ」）に対してプログラミング・インターフェースを提供する。カード・サービスは、一般には、以下のファンクションを

備えている。
(1) カード・サービス・クライアントの登録。
(2) ＰＣカードの挿入・抜き取りなどのステータスの通知。
(3) ＰＣカードに割り当てたハードウェア・リソース（例えばＰＣカードが使用するメモリ空間やＩ／Ｏ空間、割り込みレベルなど）の集中管理。
カード・サービスは、ハードウェア・リソースを管理するために、リソース・マネージメント・テーブルを内部に保有している。本実施例に係るカード・サービスは、カード・ユーティリティ・プログラム（後述）と協働的に動作することによって本発明を実現化するファンクションをさらに備えているが、この点はＤ項で説明する。
【００４８】クライアント・デバイス・ドライバは、アプリケーション・プログラム（後述）がＰＣカードを使用可能にするためのデバイス・ドライバであり、例えば日本アイ・ビー・エム（株）の「オート・コンフィギュレータ」がこれに該当する。クライアント・デバイス・ドライバは、基本的には、カード・サービスを利用して動作するクライアント・プログラムである。例えば、カード・サービスからスロット２６にＰＣカードが挿入された旨のイベントを受け取ると、クライアント・デバイス・ドライバは、ＰＣカード内に記録されたカード属性情報（「ＣＩＳ」又は「タプル」ともいう）をもとに、Ｉ／Ｏ空間と割り込みレベル（すなわちシステム・リソース）を自動的に割り当てるようになっている。リソースの割り当てを行う際、カード・サービスに対してスロット２６への電力供給の開始も要求する。ソケット・サービスは、カード・サービスからのファンクション・コールに応じて、ＰＣＭＣＩＡコントローラ２５内のレジスタ部３２の所定番地にアクセスして、電源V_{cc}及びV_{pp}からの電力供給を開始させる。また、逆にＰＣカードをスロット２６から抜き取ると、クライアント・デバイス・ドライバは、そのＰＣカードに割り当てられた全てのリソース（割り込みレベル、Ｉ／Ｏ空間、及びソケット）を解放するようになっている。リソースの解放に伴って、スロット２６への電力供給は当然停止される。
【００４９】オペレーティング・システム（ＯＳ）は、最上位層であるアプリケーション・プログラムの実行を統制するための基本ソフトウェアであり、ファイル管理、メモリ管理、タスク管理、入出力管理などのリソース管理機能や、画面表示やマウス操作の処理のためのユーザ・インターフェース（システム・コマンドとシステム・コール）を提供するものである。例えばＯＳ／２（"ＯＳ／２"は米ＩＢＭ社の商標）やＡＩＸ（"ＡＩＸ"は米ＩＢＭ社の商標）、Ｗｉｎｄｏｗｓ（"Ｗｉｎｄｏｗｓ"は米マイクロソフト社の商標）がこれに該当する。
【００５０】最上位層は、アプリケーション・プログラム（ＡＰ）であり、ユーザの意思に応じてＨＤＤ１９，ＦＤＤ２０などの補助記憶装置からメイン・メモリ１３に適宜ロードされる。本発明の実施に供されるカード・ユーティリティ・プログラムは、アプリケーション・プログラムの１つである。
【００５１】図４に示すようなソフトウェア・レイヤを備えたＰＣ１０においては、カード・サービスがクライアント・デバイス・ドライバの要求により、クライアントに対するコールバック・ルーチンと呼ばれるエントリ・ポイント（イベント・レコードをクライアントに引き渡す際の共通アドレス）を登録することで、スロット２６に装着されたＰＣカードは、ホストのシステム・コンフィギュレーションに組み込まれ、ホストからアクセスできる存在となるのである。
【００５２】Ｄ．セキュリティ・モードの設定・解除
前項までで、本発明を具現するコンピュータ・システムのハードウェア構成及びソフトウェア構成を説明してきた。本項では、該システムの動作とともに本発明の作用について説明する。
【００５３】本発明に係るパーソナル・コンピュータ１０は、ホストと装着されたＰＣカードとの間の交信を禁止するためのセキュリティ・モードを持っているが、これは、カード・サービスとカード・ユーティリティ・プログラムの協働的作用によって実現される。以下、セキュリティ・モードの設定とその解除に項分けして説明することにする。
【００５４】Ｄ－１．セキュリティ・モードの設定
図５には、セキュリティ・モードを設定するためのＰＣ１０のオペレーションをフローチャート化して示している。
【００５５】カード・スロット２６のセキュリティ・モードを設定するためには、ユーザは、まずカード・ユーティリティ・プログラムを起動する（ステップＳ１００）。カード・ユーティリティ・プログラムの起動は、マルチ・ウィンドウ画面上でユーティリティ・アイコンを開く、という形態であってもよい。
【００５６】起動したカード・ユーティリティ・プログラムは、まず、ユーザが既にパスワードを登録しているかどうかを質問する（ステップＳ１０２）。もし登録済みであれば、次ステップＳ１０４をスキップして次々ステップＳ１０６に進む。もし未登録であれば、次ステップＳ１０４に進み、ユーザに対しパスワードの入力を促し、パスワードを新規登録する。
【００５７】ステップＳ１０６では、カード・ユーティリティ・プログラムは、カード・スロット２６にＰＣカードが挿入されているかどうかを判別する。その判断結果が肯定的であれば、次ステップＳ１０８に進む。判断結果が否定的であれば、次の２ステップＳ１０８及びＳ１１０をスキップして、ステップＳ１１２に進む。
【００５８】ステップＳ１０８では、カード・ユーティリティ・プログラムは、カード・サービスに対して「擬

似カード・リムーバル・イベント」の発行を要求する。この擬似カード・リムーバル・イベントとは、ＰＣカードがスロット２６に挿入されたままであるにも拘らず、あたかもＰＣカードがスロット２６から抜き取られたことを検出したかのごとく振る舞う事象のことである。物理的には、レジスタ部３２のｎ番地のビットをリセットし、カード・スロット２６のCard Detectピンの検出レベルに拘らず該ビットのリセット状態を保つ。

【００５９】クライアント・デバイス・ドライバは、この擬似カード・リムーバル・イベントを通知されると、ＰＣカードが抜き取られたと錯覚を起こし、スロット２６のリソースを解放する（ステップＳ１１０）。スロット２６のリソースが解放された結果、スロット２６への電力供給は当然停止される。

【００６０】次いで、ステップＳ１１２では、カード・ユーティリティ・プログラムが、カード・サービスに対して、パスワード付きで、セキュリティ・モードの設定を通知する。これによってカード・スロット２６は、セキュリティ・モードに入る。カード・サービスは、受け取ったパスワードを独自に保管し、以後セキュリティ・モードの解除は、パスワード付きでなければ受け付けない（後述）。

【００６１】セキュリティ・モードにおいては、カード・スロット２６にＰＣカードが再挿入されても、カード・サービスはこれを一切無視し、クライアント・デバイス・ドライバに対してＰＣカードが挿入された旨のイベントを決して発行しない。また、クライアント・デバイス・ドライバから、スロット２６への電力供給開始やその他のサービス要求があっても、「ＰＣカードは挿入されていない」という旨の返答をするのみで、サービスを行わない。

【００６２】なお、本実施例において、セキュリティ・モードの設定をパスワード付きで行う意義は、不正なユーザによるセキュリティ・モードの勝手な解除を禁止する点にある。例えばカード・サービスのファンクション・コードを知っている不正なユーザであれば、カード・ユーティリティ・プログラムに類似したプログラムを作成し、且つシステムにロードして、カード・サービスに所望のアクション（例えばＰＣカードが挿入された旨のイベントの発行）を起こさせることも可能であろう。しかし、本実施例では、カード・サービスへのアクセスは、カード・ユーティリティ・プログラムで登録されたものと同じパスワードを伴っていなければ受付けられない。したがって、パスワードを知らない不正なユーザが他のプログラムを介して勝手にアクセスを試みても、カード・サービスは受付けないのである。

【００６３】Ｄ－２．セキュリティ・モードの解除

図６には、セキュリティ・モードを解除するためのＰＣ１０のオペレーションをフローチャート化して示している。

【００６４】カード・スロット２６のセキュリティ・モードを解除するためには、ユーザは、まずカード・ユーティリティ・プログラムを起動する（ステップＳ２００）。カード・ユーティリティ・プログラムの起動は、マルチ・ウィンドウ画面上でユーティリティ・アイコンを開く、という形態であってもよい（前述）。

【００６５】起動したカード・ユーティリティ・プログラムは、まず、ユーザに対してパスワードの入力を促す（ステップＳ２０２）。次いで、カード・ユーティリティ・プログラムは、入力されたパスワードを既に登録済みのパスワードと照合し、一致するかどうかを判断する（ステップＳ２０４）。パスワードの入力に失敗すると、分岐Ｎｏから抜けてステップＳ２１２に進む（後述）。一方、パスワードの入力が成功裡に済めば、分岐Ｙｅｓを経て次ステップＳ２０６に進む。

【００６６】次いで、ステップＳ２０６では、カード・ユーティリティ・プログラムは、カード・サービスに対して、ステップＳ２０２にて入力されたパスワード付きで、セキュリティ・モードの解除を要求する。

【００６７】次いで、ステップＳ２０８では、カード・サービスは、セキュリティ・モード解除要求に伴われた入力パスワードを、自分が保管しているパスワードと照合する。パスワードの照合に失敗すると、分岐Ｎｏから抜けてステップＳ２１２に進む（後述）。一方、パスワードの照合が成功裡に済めば、分岐Ｙｅｓを経て次ステップＳ２１０に進む。なお、カード・ユーティリティ・プログラム（ステップＳ２０４）及びカード・サービス（ステップＳ２０８）の２個所でパスワードのチェックを行う意義は、既述したように、不正なユーザがカード・ユーティリティ・プログラムに類似したプログラムによって勝手にセキュリティ・モードを解除する、ということを好適に防止して、システムの機密保護を向上できる点にある。

【００６８】次いで、ステップＳ２１０では、カード・サービスは、挿入されたＰＣカード及びクライアント・デバイス・ドライバへのサービスを再開する。この結果、カード・サービスは、クライアント・デバイス・ドライバに対して、カード・スロット２６にＰＣカードが挿入されている旨のイベントを発行する。また、クライアント・デバイス・ドライバは、ＰＣカードへの電力供給開始を命令するとともに、ＰＣカードにシステム・リソースを割り当てる。

【００６９】一方、パスワードの入力に失敗した結果として陥るステップＳ２１２では、カード・ユーティリティ・プログラム又はカード・サービスは、ユーザに対して、さらに数回（例えば2回）パスワードを再入力する機会を与える。ここで、パスワード入力に成功すると、正常なステップ（ステップＳ２０６又はＳ２１０）に復帰することができる。一方、さらにステップＳ２１２でもパスワード入力に失敗すると、パスワード入力の機会

を奪うのみならず、セキュリティ・モードをロック状態にし解除不能にしてしまう。セキュリティ・モードがロックされると、ＰＣ１０の電源を再投入（Power On Reset）しない限りは、ＰＣカードへのアクセスを行えなくなる。電源再投入の際には、ＰＣ１０内の揮発性データは当然失われてしまうので、機密データの不正な漏洩を未然に防止することができる訳である。

【００７０】Ｅ．追補

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【００７１】

【発明の効果】以上詳記したように、本発明によれば、情報処理装置は、「セキュリティ・モード」に遷移すると、現実のデバイス（ＰＣカード）の装着の有無に拘らず、あたかもデバイスが装着されていないかのように擬似的に振る舞うようになっている。したがって、セキュリティ・モード下では、装着されたＰＣカードには電力を供給せず、ＰＣカードは活動化しないことになる。この間は、当然、装着されたＰＣカードとパーソナル・コンピュータは互いに交信することはできない。

【００７２】セキュリティ・モードに設定する際に、ユーザに対してパスワードの入力を求めるようにしてもよい。また、セキュリティ・モードを解除する際にも、ユーザに対してパスワードの入力を求めるようにしてもよい。さらに、セキュリティ・モードを解除する際、所定回数以上パスワード入力に失敗するとパスワードの再入力だけでなくセキュリティ・モードの解除自体を禁止してしまうようにしてもよい。

【００７３】本発明によれば、不正なユーザが許可なくセキュリティ・モードを解除し、ＰＣカードを介してＰＣ内の機密データにアクセスする、ということはできない。したがって、１９９５年度版のＰＣＭＣＩＡ規格"ＰＣ Ｃａｒｄ Ｓｔａｎｄａｒｄ"に基づいて、ＣＰＵカードのようなバス・マスタとなり得るＰＣカードが開発される運びとなった暁に、不正なユーザがこのようなＰＣカードをＰＣ側のカード・スロットに挿入しても、セキュリティ・モードを設定してさえいれば、機密データの不正な漏洩を確実に防止することができる。

【００７４】また、本発明では、セキュリティ・モードは、ＰＣ本体がデバイスを装着していないと擬似認識することによって実現されるモードであり、デバイス側からは勝手に解除することはできない。したがって、不正なユーザが勝手にＰＣカードを差し替えてもＰＣカードからＰＣ内部に侵入することはできないのである。

【００７５】要するに本発明によれば、装着されたＰＣカードから情報処理装置内部への不正な侵入（すなわち機密データへのアクセス）を好適に防止することができる訳である。また、このような機密保護オペレーションは、ソフトウェア・レベルで実現することができるのである。

【図面の簡単な説明】

【図１】図１は、本発明の実施に供されるパーソナル・コンピュータ（ＰＣ）のハードウェア構成を示した図である。

【図２】図２は、ＰＣ１０本体とＰＣカードとを連絡するためのハードウェア構成を、より詳細に描いた図である。

【図３】図３は、レジスタ部３２の内部構成を模式的に示した図である。

【図４】図４は、ＰＣ１０のソフトウェア構成を示した図である。

【図５】図５は、セキュリティ・モードを設定するためのＰＣ１０のオペレーションをフローチャート化した図である。

【図６】図６は、セキュリティ・モードを解除するためのＰＣ１０のオペレーションをフローチャート化した図である。

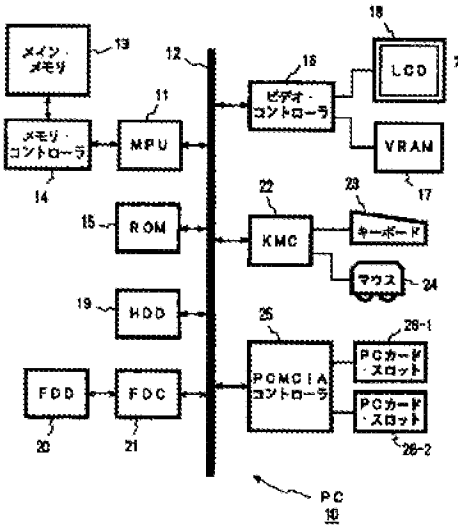
【図７】図７は、パーソナル・コンピュータにデバイスを拡張する様子を示した図であり、より具体的には、図７(a)はデスクトップ型ＰＣに拡張アダプタを装着する様子を、図７(b)にはノートブック型ＰＣにＰＣカードを装着する様子を示している。

【図８】図８は、ＰＣカードのロック機構（従来例）を示した図である。

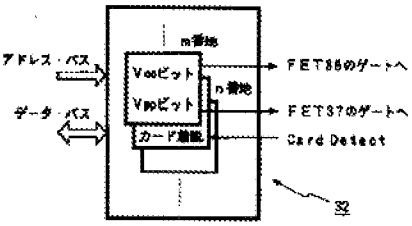
【符号の説明】

１０…パーソナル・コンピュータ（ＰＣ）、１１…ＭＰＵ、１２…バス、１３…メイン・メモリ、１４…メモリ・コントローラ、１５…ＲＯＭ、１６…ビデオ・コントローラ、１７…ＶＲＡＭ、１８…ＬＣＤ、１９…ＨＤＤ、２０…ＦＤＤ、２１…ＦＤＣ、２２…ＫＭＣ、２３…キーボード、２４…マウス、２５…ＰＣＭＣＩＡコントローラ、２６…ＰＣカード用スロット、３１…インターフェース部、３２…レジスタ部、３３…電源管理部、３４…ドライバ部、３５…レシーバ部、３６…電源コントローラ

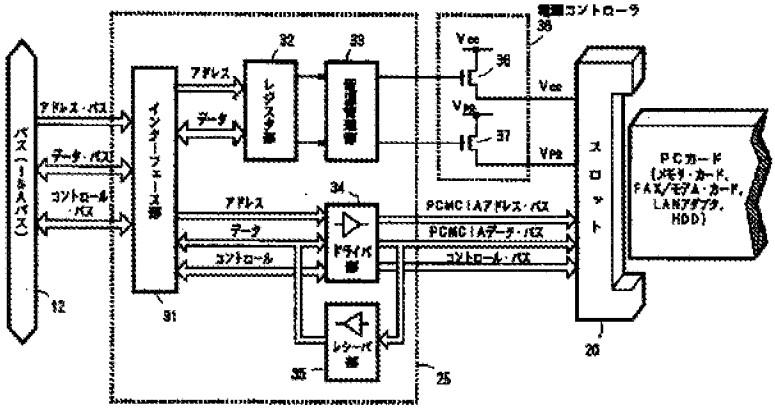
【図1】


メイン・メモリ
13
12
18
LCD
ビデオ・コントローラ
16
VRAM
17
メモリ・コントローラ
14
MPU
11
ROM
15
KMC
22
キーボード
23
マウス
24
HDD
19
FDD
20
FDC
21
25
PCMCIA コントローラ
26-1
PCカード・スロット
26-2
PC
10

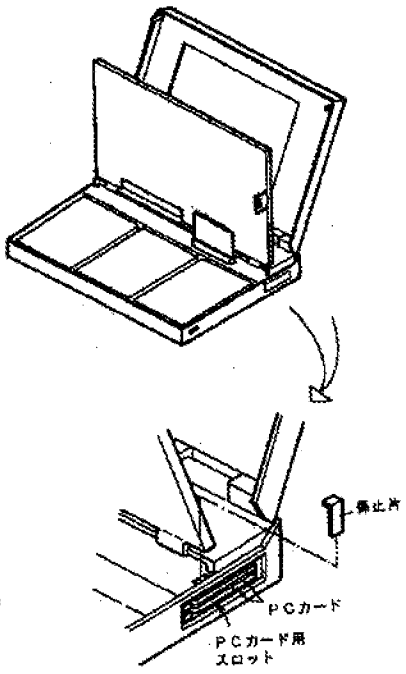
【図3】


アドレス・バス
データ・バス
m番地
Vccビット
Vppビット
n番地
カード種別
FET35のゲートへ
FET37のゲートへ
Card Detect
32

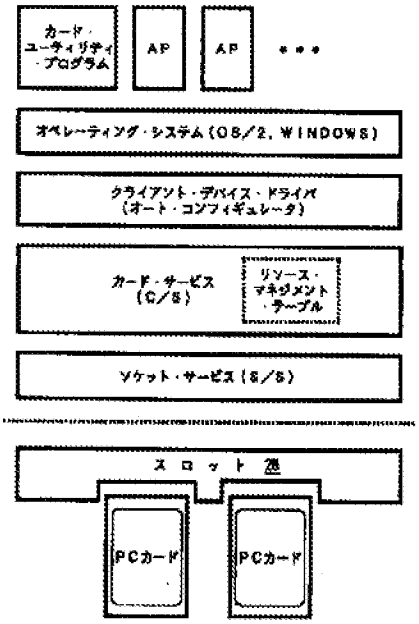
【図2】


アドレス・バス
データ・バス
コントロール・バス
バス（システムバス）
12
インターフェース部
31
アドレス
データ
32
レジスタ部
33
電圧コントローラ
36
Vcc
36
Vpp
37
Vpp
スロット
20
PCカード（メモリ・カード、FAX/モデム・カード、LANアダプタ、HDD）
34
ドライバ部
PCMCIAアドレス・バス
PCMCIAデータ・バス
コントロール・バス
レシーバ部
35
25

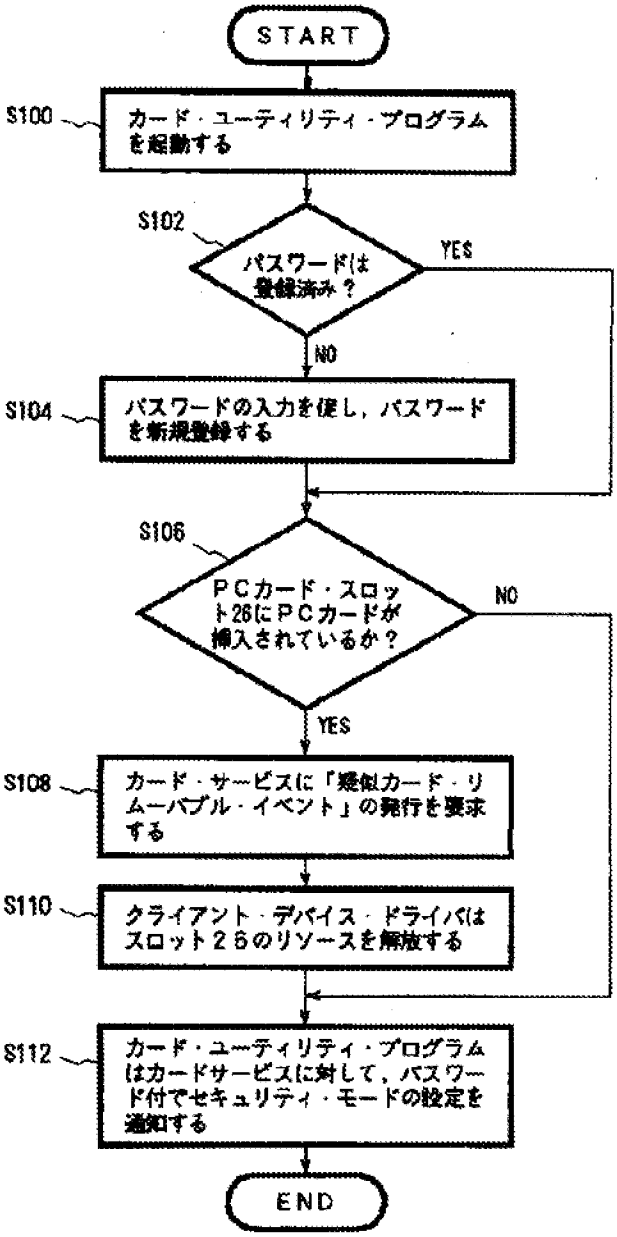
【図8】


係止片
PCカード
PCカード用スロット

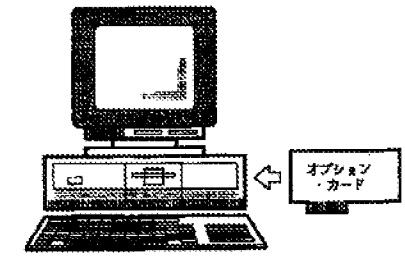
【図4】


カード・ユーティリティ・プログラム
AP
AP
・・・
オペレーティング・システム（OS/2, WINDOWS）
クライアント・デバイス・ドライバ（オート・コンフィギュレータ）
カード・サービス（C/S）
リソース・マネジメント・テーブル
ソケット・サービス（S/S）
スロット部
PCカード
PCカード

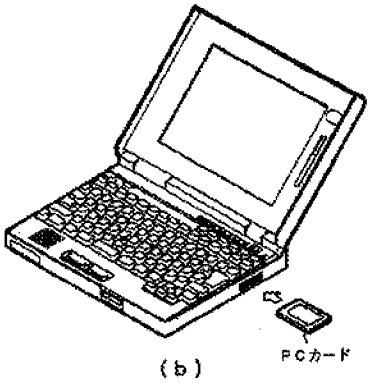
【図5】


START
S100
カード・ユーティリティ・プログラムを起動する
S102
パスワードは登録済み？
YES
NO
S104
パスワードの入力を促し，パスワードを新規登録する
S106
PCカード・スロット26にPCカードが挿入されているか？
NO
YES
S108
カード・サービスに「疑似カード・リムーバブル・イベント」の発行を要求する
S110
クライアント・デバイス・ドライバはスロット26のリソースを解放する
S112
カード・ユーティリティ・プログラムはカードサービスに対して，パスワード付でセキュリティ・モードの設定を通知する
END

【図7】

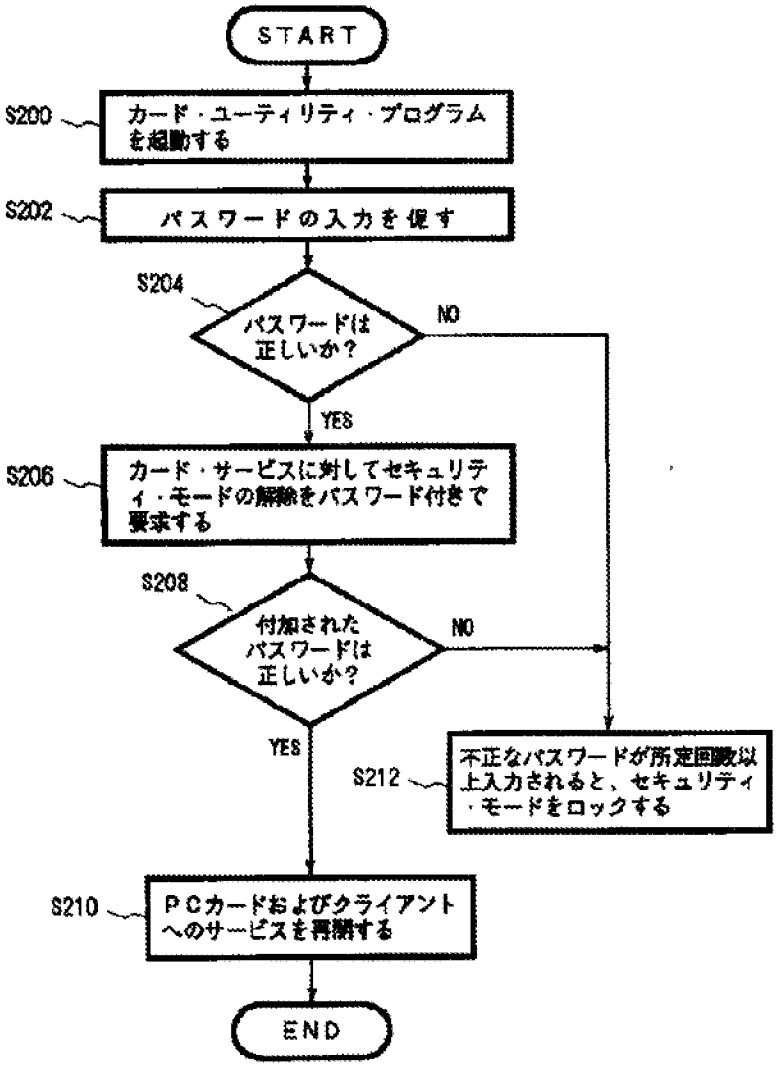

オプション・カード

（a）


PCカード

（b）

【図6】



【手続補正書】
【提出日】平成８年２月２６日
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【特許請求の範囲】
【請求項１】デバイスを装着するための接続部を持ち、且つ装着されたデバイスに対して電力を供給するタイプの情報処理装置において、所定の動作モード下では、装着されたデバイスに対する電力供給を停止可能なことを特徴とする情報処理装置
【請求項２】デバイスを装着するための接続部を持ち、且つ該接続部へのデバイスの装着を検出すると該デバイスに電力供給を行うタイプの情報処理装置において、所定の動作モード下では、デバイスの装着の有無に拘らず該接続部からの電力供給を停止することを特徴とする情報処理装置
【請求項３】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持ち、該検出部の検出結果に応じて装着されたデバイスに電力供給を行うタイプの情報処理装置において、所定の動作モード下では、前記検出部の検出結果に拘らず擬

似的にデバイスが装着されていないと判断してデバイスへの電力供給を停止することを特徴とする情報処理装置

【請求項4】デバイスを装着するための接続部を持ち、且つ装着されたデバイスとの間で交信可能なタイプの情報処理装置において、所定の動作モード下では、装着されたデバイスとの交信を禁止することを特徴とする情報処理装置

【請求項5】デバイスを装着するための接続部を持ち、且つ該接続部へのデバイスの装着を検出すると該デバイスとの交信が可能になるタイプの情報処理装置において、所定の動作モード下では、デバイスの装着の有無に拘らずデバイスとの交信を禁止することを特徴とする情報処理装置

【請求項6】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持ち、該検出部の検出結果に応じて装着されたデバイスとの交信が可能になるタイプの情報処理装置において、所定の動作モード下では、前記検出部の検出結果に拘らず擬似的にデバイスが装着されていないと判断して交信を禁止することを特徴とする情報処理装置

【請求項7】入力されたパスワードの照合結果に応じて前記所定の動作モードに遷移することができることを特徴とする請求項1乃至請求項6のいずれかに記載の情報処理装置

【請求項8】入力されたパスワードの照合結果に応じて前記所定の動作モードから抜け出すことができることを特徴とする請求項1乃至請求項6のいずれかに記載の情報処理装置

【請求項9】前記所定の動作モードとは機密保護性の高いセキュリティ・モードであることを特徴とする請求項1乃至請求項6のいずれかに記載の情報処理装置

【請求項10】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持つタイプの情報処理装置の制御方法において、所定の動作モード下では、前記検出部の検出結果に拘らず前記接続部にはデバイスが装着されていないものと判断することを特徴とする情報処理装置の制御方法

【請求項11】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持つタイプの情報処理装置の制御方法において、所定の動作モード下では、前記検出部の検出結果に拘らず前記接続部にはデバイスが装着されていないものと判断して、装着されたデバイスへの電力供給を停止することを特徴とする情報処理装置の制御方法

【請求項12】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持つタイプの情報処理装置の制御方法において、所定の動作モード下では、前記検出部の検出結果に拘らず前記接続部にはデバイスが装着されていないものと判断して、装着されたデバイスとの交信を禁止することを特徴とする情報処理装置の制御方法

【請求項13】入力されたパスワードの照合結果に応じて前記所定の動作モードに遷移することができることを特徴とする請求項10乃至請求項12のいずれかに記載の情報処理装置の制御方法

【請求項14】入力されたパスワードの照合結果に応じて前記所定の動作モードから抜け出すことができることを特徴とする請求項10乃至請求項12のいずれかに記載の情報処理装置の制御方法

【請求項15】前記所定の動作モードとは機密保護性の高いセキュリティ・モードであることを特徴とする請求項10乃至請求項12のいずれかに記載の情報処理装置の制御方法

【請求項16】パスワードの入力に所定回数以上失敗すると前記所定の動作モードの解除を禁止してしまうことを特徴とする請求項7に記載の情報処理装置

【請求項17】パスワードの入力に所定回数以上失敗すると前記所定の動作モードの解除を禁止してしまうことを特徴とする請求項14に記載の情報処理装置の制御方法

【請求項18】デバイスを装着するための接続部を持ち、且つ装着されたデバイスに対してシステム資源を割り当てるタイプの情報処理装置において、所定の動作モード下では、装着されたデバイスに対して割り当てたシステム資源を解放することを特徴とする情報処理装置

【請求項19】デバイスを装着するための接続部を持ち、且つ該接続部へのデバイスの装着を検出すると該デバイスにシステム資源を割り当てるタイプの情報処理装置において、所定の動作モード下では、デバイスの装着の有無に拘らず該デバイスに割り当てたシステム資源を解放することを特徴とする情報処理装置

【請求項20】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持ち、該検出部の検出結果に応じて装着されたデバイスにシステム資源を割り当てるタイプの情報処理装置において、所定の動作モード下では、前記検出部の検出結果に拘らず擬似的にデバイスが装着されていないと判断してデバイスに割り当てたシステム資源を解放することを特徴とする情報処理装置

【請求項21】デバイスを装着するための接続部と該接続部へのデバイスの装着の有無を検出するための検出部を持つタイプの情報処理装置の制御方法において、所定の動作モード下では、前記検出部の検出結果に拘らず前記接続部にはデバイスが装着されていないものと判断して、装着されたデバイスに割り当てたシステム資源を解放することを特徴とする情報処理装置の制御方法

フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	F I		技術表示箇所
G06K 17/00			G06F 1/00	334C	

(72)発明者　篠村　正彦
神奈川県大和市下鶴間1623番地14　日本アイ・ビー・エム株式会社　大和事業所内